Don Springmeyer, Esq. (#1021)
Michael J. Gayan, Esq. (#11135)
Kemp Jones, LLP
3800 Howard Hughes Parkway, 17th Floor
Las Vegas, NV 89169
Tel: (702) 385-6000
d.springmeyer@kempjones.com
Liaison Counsel

John A. Yanchunis
Morgan & Morgan
Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com
Interim Class Counsel

Douglas J. McNamara
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW, 5th Floor
Washington, D.C. 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com
Interim Class Counsel

Amy Keller
DiCello Levitt LLP
10 North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Tel: (312) 214-7900
akeller@dicellolevitt.com
Interim Class Counsel

Counsel for Plaintiffs and the Class

(Additional Counsel Listed on Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

In re: DATA BREACH SECURITY LITIGATION AGAINST CAESARS ENTERTAINMENT, INC.

Case No. 2:23-cv-01447-ART-BNW

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulatory Authorities

Other Authorities

Rules

Defendant, Caesars Entertainment, Inc. ("Caesars" or "Defendant"), collects personal information on hundreds of millions of people, mining it for profit. But instead of taking the necessary and reasonable steps to secure that personal information from well-known threats, Caesars allowed financially motivated hackers access to it. Now, criminals are using Plaintiffs' private information target them for identity theft and other misuse. Plaintiffs also face substantial risk of future harm.

Caesars' motion to dismiss parrots the standard arguments raised in data breach cases, even when those arguments do not fit the facts Plaintiffs allege. Caesars repeatedly ignores the actual allegations in the Complaint and misstates or omits critical holdings in relevant cases. The Court should deny Caesars' motion in its entirety.[1]

I. BACKGROUND

On or around August 18, 2023, members of the cybercriminal group Scattered Spider called Caesars' IT vendor pretending to be a Caesars' employee and requested the employee's login credentials be reset. *See* Consolidated Class Action Complaint ("CAC"), ECF No. 81, ¶¶ 2, 224, 225. Caesars claims it learned of the attack that day, and "activated [its] incident response protocols" and "implemented a series of containment and remediation measures." Caesars Entertainment, Inc. Form 8-K, Report of unscheduled material events or corporate event, at 2 (Sept. 14, 2023), available at https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57. Yet, five days later, the cybercriminal used the provided credentials to download a copy of Caesars' loyalty program database ("Data Breach"). CAC ¶ 225. The database included the sensitive Personally Identifiable Information ("PII") including the names, driver's license, and social security numbers of Plaintiffs and a "significant number" of the 65 million members of Caesars loyalty program from Caesars's inadequately protected servers. *Id.* ¶ 1. Caesars concealed the Data Breach until September 14, 2023. *Id.* ¶ 228. Plaintiffs represent putative classes of consumers harmed Caesars' failure to adequately secure and protect their PII. *Id.* ¶¶ 308, 312.

[1] Plaintiffs have sought an extension of the page limits for their brief, which is unopposed. *See* ECF No. 95. And Caesars previously sought an extension of the page limits for their motion, Plaintiffs' brief, and its reply. ECF No. 89. To the extent the Court does not grant those motions, Plaintiffs respectfully request that they be provided an opportunity to respond to any motion that Caesars files within the page limits provided by the Local Rules.

A. Aware of the Risks, Caesars Fails to Protect Plaintiffs' and Class Members' PII From Dangerous Cybercriminals

Caesars is one of the world's largest and most sophisticated lodging and gaming companies. *Id.* ¶ 3. Its loyalty program, Caesars Rewards, allows its 65 million members to earn redeemable credits by gambling or staying at Caesars properties. *Id.* ¶¶ 3-4, 210. Caesars requires its rewards members to provide highly sensitive PII such as their full legal name, full address, date of birth, drivers' license number, and Social Security number. *Id.* ¶ 212. Caesars profits from this data—using it for marketing purposes and to develop new products and services. *Id.* ¶ 282. Caesars knows rewards members value information security, and induces them to provide it by promising to "maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control." *Id.* ¶ 239.

Here, Caesars failed to keep this promise. It did not comply with established cybersecurity frameworks or industry standards to protect the Plaintiffs' and Class Members' PII it collected even though it knew that it faced a serious threat from cybercriminals. *Id.* ¶¶ 250, 251, 259. It knew that several of its competitors experienced data breach incidents recently because the type of PII collected by the hospitality industry makes it particularly appealing to cyber criminals. *Id.* ¶¶ 243, 246. Caesars told its investors in 2022 that cyberattacks were a significant risk factor it faced, and that a data breach of its "customers' personal information could materially harm our reputation and business." *Id.* ¶ 250.

Scattered Spiders' ability to infiltrate Caesars's servers and exfiltrate the PII of tens of millions of customers through "convincing phone calls" demonstrates Caesars' failure to comply with reasonable and adequate cybersecurity practices. *Id.* ¶ 2. After the Data Breach, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA). *Id.* ¶ 265. The CSA detailed established cybersecurity mitigation techniques to protect against the social engineering techniques used by Scattered Spider. *Id.* ¶ 266. Caesars did not implement all of these techniques, leading to the Data Breach. *Id.* ¶ 267.

B. Caesars' Cybersecurity Failures Led Directly to Plaintiffs' Harm

Caesars' failure to protect rewards customers' PII injured Plaintiffs and Class Members in several ways. First, Plaintiffs incurred financial losses and continue to face a considerable risk of misuse

of their PII from the Data Breach because their PII is now in the hands of "one of the most dangerous financial criminal groups." *Id.* ¶ 58. They have endured actual and attempted fraud and/or have been exposed to an increased risk of fraud, identity theft, and other misuse of their PII. *Id.* ¶ 10. They must now and indefinitely closely monitor their financial and other accounts to guard against fraud. *Id.* To protect themselves from this increased risk of fraud, they have or will buy credit monitoring and other identity protection services, purchase credit reports, place credit freezes and fraud alerts on their credit reports, and spend time investigating and disputing fraudulent or suspicious account activity. *Id.* One Plaintiff has already spent $400 for a one-year subscription for identity protection services. *Id.* ¶ 16.

A number of Plaintiffs have already discovered that their PII was for sale on the Dark Web following the Data Breach. *Id.* ¶ 6, 20, 41, 51, 61, 82, 92, 118, 122, 140, 170, 191, 273. The stolen PII can be misused on its own or can be combined with personal information from other sources (such as publicly available information, social media) to create a package of information capable of being used to commit further identity theft. *Id.* ¶ 11. Thieves can also use the stolen PII to send spear-phishing emails and text messages to Class Members to trick them into revealing sensitive information such as Social Security numbers, financial account numbers, login credentials, and the like. *Id.*

Caesars claimed that it had taken "steps to ensure that the stolen data *is* deleted by the unauthorized actor, *although [it] cannot guarantee this result.*"[2] Caesars never identified the "steps" that it took nor confirmed that the stolen data *was* deleted. News reports claimed that Scattered Spider received a ransom of $15 million dollars to supposedly delete the data. CAC ¶ 226. But Caesars has never confirmed this report in any public statement or regulatory filing. Even if true, as Caesars made clear, it cannot guarantee that the stolen data is deleted. This is especially true when Scattered Spider is known to have exfiltrated stolen data to "multiple sites included U.S.-based data centers and MEGA.NZ." *Id.* ¶ 271. Moreover, according to a Government Accountability Office Report, the threat of future identity theft lingers for a long time after a data breach given the time lag between when information is stolen and when it is used. *Id.* ¶ 296. In some cases, "stolen data may be held for

[2] Caesars Entertainment, Inc. Form 8-K, Report of unscheduled material events or corporate event, at 2 (Sept. 14, 2023) (emphasis added), available at https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57.

up to a year or more before being used to commit identity theft[,]" and "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." *Id.* [3]

Second, Plaintiffs and Class Members have also suffered "benefit of the bargain" damages because they paid money to Caesars for services that were intended to include adequate data security but did not. Plaintiffs would not have stayed at Caesars hotels or would have paid less for their rooms if they had known the truth about Caesars' deficient data security practices. *Id.* ¶ 290

Third, Plaintiffs and Class Members also suffered a "loss of value of PII" resulting from the Data Breach. *Id.* ¶¶ 276-285. The value of personal information is increasingly evident in our digital economy as shown by companies, including Caesars, collection of personal information for purposes of data analytics and marketing. *Id.* ¶ 282. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. *Id.* ¶ 284. The value of PII is derived not from a price at which consumers seek to sell it, but from the economic benefit consumers derive from using it. *Id.* A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. *Id.*

II. STANDARD OF REVIEW

Fed. R. Civ. P. 12(b)(6). To survive dismissal, a complaint must "contain[] enough facts to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 696 (2009) (citation omitted). A complaint or individual claim should be dismissed without leave to amend only when "it is clear ... that the complaint could not be saved by any amendment." *Steckman v. Hart Brewing, Inc.*,143 F.3d 1293, 1296 (9th Cir. 1998).

Fed. R. Civ. P. 12(b)(1). Article III standing requires an injury in fact that is traceable to the challenged conduct and redressable by a favorable ruling. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). A plaintiff has suffered an injury in fact if she has "suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 339 (cleaned up). A Rule 12(b)(1) jurisdictional challenge may be facial or factual. *Safe Air for*

[3] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, United States Government Accountability Office (June 2007), (last visited July 19, 2024).

Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). In a facial attack, like Caesars', "the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction." *Id.* When evaluating a facial challenge, the court must assume the truth of the allegations and draw all reasonable inferences in plaintiffs' favor. *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004).

III. ARGUMENT

A. Plaintiffs Adequately Plead Article III Standing.

Beyond Caesars' fleeting contention related to traceability in the limited context of Plaintiffs' alleged cognizable injury of attempted fraud, Mot. at 8-10, the crux of Caesars' standing argument challenges the injury-in-fact element. *Id.* at 1-2, 6-13. All other elements are indisputably established. As demonstrated below, Caesars misrepresents Plaintiffs' allegations, and misstates precedents in a failed attempt to contradict Article III standing. Caesars bolsters flawed arguments with immaterial case citations that generally stand for the uncontroversial proposition that Plaintiffs must adequately allege damages resulting from a data breach. Plaintiffs have met their burden of establishing standing.

1. Plaintiffs Adequately Allege Concrete and Particularized Injuries Constituting Injury-in-Fact for Purposes of Article III Standing.

In this Circuit, a plaintiff establishes injury-in-fact sufficient for Article III standing in data breach cases by demonstrating a credible threat of real and immediate harm stemming from the theft of their personal information, even if the information has not yet been misused. *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) (citing *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010)). The Ninth Circuit evaluates the sensitivity of the personal information, combined with its theft, in order to determine whether the plaintiffs had adequately alleged an injury in fact supporting standing. *Zappos*, 888 F.3d at 1027. For instance, in *Krottner*, a thief stole a laptop containing "the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees." 628 F.3d at 1140. The Ninth Circuit held that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." 628 F.3d at 1143. In *Zappos*, the Ninth Circuit held that the sensitivity of the alleged stolen PII data (account numbers, passwords, etc.) required the same conclusion as in *Krottner* based on a substantial

risk of identity fraud or identity theft. 888 F.3d at 1029.

Caesars falsely contends that Plaintiffs do not allege any injuries sufficient for Article III standing. Mot. at 1-2. Plaintiffs allege the "crown jewels" of PII—including driver's license numbers, and Social Security numbers—were stolen by criminals in the Breach. CAC ¶¶ 227, 229. Moreover, Plaintiffs allege that their "highly sensitive" PII has already been found on the Dark Web and that their compromised PII has already been misused and exploited for fraud. *Id.* ¶¶ 233, 271, 273. Plaintiffs further (1) actual and attempted fraud and identity theft; (2) lost value of their PII; (3) overpayment for Caesars' services that were intended to be accompanied by adequate data security but were not; (4) expenses and lost time related to mitigation efforts to protect themselves from fraudulent activity made necessary by the Data Breach; and (5) increased, imminent risk of fraud and identity theft and other misuse of their PII. *See, e.g.*, CAC ¶¶ 10, 407. These allegations squarely place this case in the vein of *Zappos* and *Krottner*.[4]

a. Allegations of actual or attempted fraud demonstrate standing.

First, there is no question that allegations of fraud, attempted fraud, identity theft, and misuse of PII satisfy Article III's standing requirement. *See, e.g.*, CAC ¶ 71-72 ("In addition, as a result of the Data Breach, Plaintiff Gedwill has experienced a phishing attempt in which a stranger sent him money and requested that he return it. Plaintiff Gedwill also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach."); *id.* ¶ 340 ("There is a temporal and close causal connection between Caesars' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs"). Rather than argue that Plaintiffs have not met their burden to proceed in federal court, Caesars instead argues that Plaintiffs' allegations are not specific enough or that Plaintiffs "cannot plausibly connect" the fraud to Caesars' breach. Mot. at 1-2. Caesars' argument inappropriately conflates the pleadings

[4] Caesars cites to *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), but this is not a situation where sensitive information *may* be disclosed to a third party in the future. Here, criminals *already* have the data that Caesars had a duty to protect. *Accord Medoff v. Minka Lighting, LLC*, 2023 WL 4291973, at *3 (C.D. Cal. May 8, 2023) (finding that plaintiff had established standing through "loss of control of his PII and the subsequent exposure of this PII to the dark web" and because he "faces an imminent risk of identity theft or fraud as a result of the data breach").

stage with summary judgment, and should be disregarded. *See Zappos*, 888 F.3d at 1028.

b. Loss of value of PII is an acceptable damages theory for standing.

Plaintiffs have also established standing related to their allegations concerning loss of value and control over their PII. CAC ¶¶ 18, 29, 50, 235-37, 282-285. In a recent and analogous case involving a data breach of a casino, the district court determined that Plaintiffs had stated a cognizable damages theory related to the valuation of PII sufficient to survive defendant's motion to dismiss. *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1190 (D. Nev. 2022). Other courts in this Circuit have agreed. *See, e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *12-13 (N.D. Cal. Aug. 30, 2017); *In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations of harm from the dissemination of their personal information and loss of sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (collecting cases recognizing lost property value).

c. Plaintiffs' "overpayment theory satisfies Article III.

Plaintiffs sufficiently allege that they did not receive the benefit of their bargain with Caesars sufficient to demonstrate standing. As the Ninth Circuit has held repeatedly, when Plaintiffs "contend that [they] paid more for [a service] than they otherwise would have paid, or bought it when they otherwise would not have done so they have suffered an Article III injury in fact." *Bowen v. Energizer Holdings, Inc.*, 2024 WL 4352496, at *7-8 (9th Cir. Oct. 1, 2024) (cleaned up). This is often referred to as an "overpayment theory." *Id.* (cleaned up). A plaintiff proceeding on an overpayment theory of Article III standing typically must "allege that [the defendant] made false representations—or actionable non-disclosures—about [the product or service]." *Id.* (citing *McGee v. S-L Snacks Nat'l*, 982 F.3d 700, 707 (9th Cir. 2020)).

Many district courts within the Ninth Circuit have held that "general allegations" providing that data security was expected and was part of the bargain is enough to sufficiently allege that plaintiffs suffered benefit-of-the-bargain losses. Similar to the *MGM* case, Plaintiffs allege that they overpaid for Caesars' services that should have been—but were not—accompanied by adequate data security.

638 F. Supp. at 1189-90. *See* CAC ¶ 287 ("Part of the price consumers paid to Caesars was intended to be used to provide adequate data security. … Indeed, if consumers did not value data security and privacy, Caesars would have no reason to tout its data security efforts in its Privacy Policy."), ¶ 288-291 (had "consumers known the truth about Caesars' deficient data security practices, they would not have stayed at Caesars properties or would have paid less than they did for their rooms"). As in the *MGM* case, that Plaintiffs have sufficiently alleged benefit of the bargain damages.

d. Plaintiffs' mitigation efforts were reasonable and confer standing.

Plaintiffs incurred reasonable, and necessary, out-of-pocket losses because of the data breach. *See, e.g., In re Experian Data Breach Litig.*, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016) ("[t]he time that Plaintiffs have allegedly spent addressing issues caused by the data breach are thus sufficient to state a claim for damages"); *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130 (2021) (finding plaintiffs' efforts to protect their PII and the subsequent financial and time costs were sufficient to establish standing). Courts have also recognized "time spent responding to a data breach" as a non-economic injury. *Stasi* v. *Inmediata Health Grp. Corp*, 501 F. Supp. 3d 898, 913, 917(S.D. Cal. 2020) (finding "it is reasonable to infer that upon receiving notice of the breach," plaintiffs would respond by ensuring that "they had not, and would not, become victims of identity theft"). *See also In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021) (finding that plaintiffs also demonstrate standing via their mitigation efforts and purchasing identity theft protection and monitoring in data breach where Social Security numbers were exposed); *In re Accellion, Inc. Data Breach Litig.*, 713 F. Supp. 3d 623, 637 (N.D. Cal. 2024) (finding that time spent responding to a data breach is a non-economic injury that can support standing).

Without citation, Caesars argues that the mitigation efforts taken by Plaintiffs took in response to the breach are "unreasonable." Mot. at 8. Caesars also attempts to argue that, because Caesars has offered Plaintiffs "two years" of complimentary credit and dark web monitoring and due to the mere existence of a $1 million insurance reimbursement policy, Plaintiffs are wholly precluded from establishing any injuries based on (1) risk of fraud or (2) out-of-pocket costs or time spent on mitigation. Mot. at 7-8. Plaintiffs, however, may reasonably choose to purchase identity protection

services above what has been offered by Caesars, both to obtain additional protection and because of understandable skepticism about using credit monitoring provided by the company that could not keep their data secure in the first place. *See Castillo v. Seagate Tech., LLC*, 16-cv-1958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) (finding cognizable injury where plaintiffs purchased identity protection services "because they wanted greater protection than that offered by [Defendant]").

Here, Plaintiffs specifically allege in the Complaint that "they may not see the full extent of identity theft or misuse of their personal information for years to come" and that they each "face an ongoing risk and must vigilantly monitor their financial and other accounts indefinitely." CAC ¶ 298. Caesars cannot self-servingly credit its offered monitoring package as foreclosing standing.

e. Plaintiffs allege imminent and substantial ongoing risk of future injury as a result of the Data Breach.

Finally, Plaintiffs satisfy the "injury in fact" requirement because they face a real, ongoing risk of harm as a result of the data breach. Unlike *Clapper*, the future risk of harm Plaintiffs face is not "conjectural or hypothetical" because of the type of information involved in the data breach. *See Krottner*, 628 F.3d at 1143 (finding that plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted" names, addresses, and Social Security numbers). *See also Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1227 (N.D. Cal. 2022) ("the injury-in-fact requirement will be satisfied when highly sensitive personal data, such as social security numbers and credit card numbers, are inappropriately revealed to the public and increase the risk of immediate future harm to the plaintiff.")

Here, too, Plaintiffs have alleged that their highly sensitive PII, including their driver's license numbers and Social Security numbers were compromised in the Data Breach, along with a significant number of the tens of millions fellow Caesars Rewards' members. CAC ¶¶ 227, 229. In addition, Plaintiffs allege that their "highly sensitive" PII has already been found on the Dark Web and that their compromised PII has already been misused and exploited for fraud. CAC ¶¶ 233, 271, 273. These allegations satisfy the injury-in-fact requirement.

2. Caesars does not seriously challenge traceability of Plaintiffs' injuries to the data breach.[5]

Caesars challenges whether Plaintiffs' fraud-related injuries are "fairly traceable" to the Breach. Mot. at 7-9. But traceability cannot be reasonably disputed given the type of data involved, when the breach occurred, and when Plaintiffs' fraud-related injuries occurred. While Caesars demands that Plaintiffs show every link in the causal chain, Mot. at 8-9, "[p]roximate causation is not a requirement of Article III standing, which requires only that the plaintiff's injury be fairly traceable to the defendant's conduct." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014); *Wash. Env't Council v. Bellon*, 732 F.3d 1131, 1141-42 (9th Cir. 2013) (A "causal chain does not fail simply because it has several links, provided those links are not hypothetical or tenuous and remain plausible.") (citation omitted). Here, "[g]iven the scope and sensitivity of the stolen PII, it is reasonable to infer that such information could plausibly have been used to commit the fraud that [plaintiffs] suffered." *In re Sequoia Benefits & Ins. Data Breach Litig.*, WL 1091195, at *2 (N.D. Cal. Feb. 22, 2024). *See also Baton v. Ledger SAS*, 2024 WL 3447511, at *14 (N.D. Cal. July 16, 2024) (finding traceability where the "foreseeable result of [defendant's] inadequate security measures is that [defendant] would be hacked, subjecting Plaintiffs to phishing attacks.").

Plaintiffs allege that, after the Breach, their information was misused or exploited to commit fraud. CAC ¶¶ 233, 271, 273. Plaintiffs' Social Security numbers were exposed in the breach, and several Plaintiffs had credit cards opened in their name without their knowledge or consent. *Id.,* CAC ¶ 151. *See In re Equifax Inc.*, 999 F.3d at 1263 (finding "no dispute" that plaintiffs satisfied standing when they suffered fraud and identity theft after Social Security numbers were stolen in a breach). Even Caesars acknowledges that the alleged payment of the criminals' ransom demand—a fact which Caesars, itself, has never confirmed—could not guarantee that the information stolen would be deleted. Mot. at 9. These allegations demonstrate traceability.

[5] Caesars has not challenged redressability. The Court may certainly fashion relief to redress the injuries alleged by Plaintiffs. *See Zappos*, 888 F.3d at 1030 ("The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation.").

3. Plaintiffs Have Standing to Seek Injunctive Relief

Plaintiffs have standing to seek injunctive relief because they have alleged actual and imminent harm caused by Caesars' inadequate security protocols that remain in place today. They are seeking specific injunctive relief to address those harms—importantly—because *Caesars continues to hold their data*. CAC ¶¶ 304-305, 306 ("These measures are necessary to guard against future data breaches at Caesars involving Class Members' PII *that Caesars continues to retain*.") (emphasis added). That confers standing. *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 698 (N.D. Cal. 2019) (denying challenge to standing in a data breach case even where defendant had "fixed the bug that caused the data breach," because defendant's "repetitive losses of users' privacy supplies a long-term need for supervision"). Caesars' motion does not address their continued possession of Plaintiffs' data. Plaintiffs have described precisely why Caesars' actions leave them at continued risk of harm and how injunctive relief would mitigate that harm.

4. Plaintiffs Adequately Allege Damages for Their Common Law Claims

The same injuries alleged that sufficed for standing also demonstrate common law damages. These include (1) actual and attempted fraud and identity theft; (2) lost value of their PII; (3) overpayment for Caesars' services; (4) expenses and lost time related to mitigation efforts; and (5) increased, imminent risk of fraud and identity theft and other misuse of their PII. While Caesars mischaracterizes Plaintiffs damages as "speculative," Mot. at 13, it ignores that Plaintiffs have alleged that their PII has already been found on the Dark Web, and that Plaintiffs have experienced measurable increases in targeted identity theft attempts. CAC ¶¶ 6, 20, 41, 51, 61, 82, 92, 118, 122, 140, 191, 273. Further, Plaintiffs have already suffered identity theft attempts, fraudulent charges, and inquiries to credit reports, among other things. *See, e.g.*, *id.* ¶¶ 17-19, 29-30, 38, 40, 100-102, 151. These allegations not only show that Plaintiffs are at risk of identity theft, but also that Plaintiffs have suffered a loss of the value of their PII. *See id.*¶ 284. *MGM*, 638 F. Supp. 3d at 1191 ("the Data Breach devalued Plaintiffs' PII by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace. Accordingly, … Plaintiffs' have stated a cognizable theory of damages as a matter of law.").

Caesars' argument as to mitigation-related damages is also deficient. First, courts in this Circuit

have acknowledged that loss of time constitutes damages. *Stasi*, 501 F. Supp. 3d at 916-18; *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1296 (S.D. Cal. May 7, 2020). Plaintiffs have alleged that they spent significant time dealing with the Breach. CAC ¶¶ 17, 28, 49, 59, 148, 160, 169, 199. Second, Caesar omits that Plaintiffs Martin and Gill allege out-of-pocket costs by purchasing a credit monitoring service after the Data Breach. *Id.* ¶¶ 16-17, 121. Additionally, Plaintiff Martin incurred costs to change his phone number after being bombarded with spam calls and texts because of the Data Breach. *Id.* ¶ 121.

B. Plaintiffs Adequately Allege Negligence.

Plaintiffs adequately alleged a claim for negligence under Nevada law because they were harmed by Caesars' breach of its duty to protect their PII.[6]

1. Caesars Had a Duty to Protect Plaintiffs' and Class Members' PII

The proper question is not, as Caesars argues, whether Caesars owed Plaintiffs a legal duty to protect against unforeseen acts of a criminal party. Mot. 14-15. The proper question is whether Caesars had a duty to protect their PII once Caesars collected it, and the answer is "yes". Plaintiffs allege Caesars' obligations were created by the FTC Act, state law, industry standards, and representations made to Plaintiffs and Class Members. CAC ¶ 219.

a. Caesars Collection of PII created a Duty.

Courts have repeatedly recognized the existence of a duty by businesses that solicit and collect sensitive data to exercise reasonable care by taking measures to avoid a foreseeable risk of harm from a data breach incident. *See, e.g., MGM*, 638 F. Supp. 3d at 1188 (denying motion to dismiss where plaintiffs alleged defendant breached its "duty of care in their manner of collecting, maintaining, and controlling their customers' sensitive personal and financial information"); *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017)("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information"); *see also In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d

[6] Under Nevada law, a negligence claim requires "four elements: (1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages." *Sanchez v. WalMart Stores, Inc.*, 125 Nev. 818, 824 (2009).

1295, 1325 (N.D. Ga. 2019) (a duty of care to safeguard customer PII when defendant "knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures"). Foreseeability is "determined from all of the circumstances present." *Doud v. Las Vegas Hilton Corp.*, 864 P.2d 796, 800 (Nev. 1993).

Here, Caesars collected and stored a "treasure trove" of unencrypted PII. CAC ¶ 233. The risks involved in collecting and storing PII were foreseeable to Caesars. Just months before the Data Breach, Caesars told its investors in a regulatory filing that cyberattacks were a significant risk factor as a data breach of its "customers' personal information could materially harm [its] reputation and business." CAC ¶ 250. Caesars was also aware that several of its competitors had experienced data breaches in recent years, and that as many as 15-20% of data breaches occurred within the hospitality industry. CAC ¶¶ 244-45. Thus, Caesars had a duty to comply with established cybersecurity frameworks, law, and industry standards to protect that PII. CAC ¶ 218.

b. Caesars has a "special relationship" obliging it to protect customers' PII.

A special relationship exists "when " the ability of one of the parties to provide for his own protection has been limited in some way by his submission to the control of the other." *Scialabba v. Brandise Const. Co.*, 921 P.2d 928, 930 (Nev. 1996). The controlling party must take "reasonable precautions to protect" the submitting party from foreseeable criminal acts of a third party. *Id.* Nevada courts consider a variety of factors when determining whether a criminal act by a third party was foreseeable, including past experiences, the frequency of the type of crime, and the nature and quality of the business. *Barreras v. Harrah's Laughlin, Inc.*, 2005 WL 8166203, at *5 (D. Nev. Jan. 24, 2005). Special relationships include, *inter alia,* landowner-invitee, businessman-patron, and as pointed out by Caesars, innkeeper-guest. *Id.*; Mot. at 15 (citing Restatement (Second) of Torts § 314A(1)(a)).

Although the Nevada Supreme Court has not considered whether an obligation to keep PII safe would constitute a special relationship, courts elsewhere recognize a special relationship and resulting exception to the economic loss doctrine in data breach litigation. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1172 (D. Minn. 2014); *In re Equifax, Inc.*, 362 F. Supp. 3d at 1321. As the Ninth Circuit, interpreting Nevada law, has remarked, "[a] fiduciary relationship is deemed to

exist when one party is bound to act for the benefit of the other party," and the "essence" of the relationship involves parties who "do not deal on equal terms, since the person in whom trust and confidence is reposed and who accepts that trust and confidence is in a superior position to exert unique influence over the dependent party." *Giles v. GMAC*, 494 F.3d 865, 880-81 (9th Cir. 2007) (cleaned up).

Here, when Plaintiffs entrusted their PII to Caesars, an innkeeper, they relinquished all control over that information and placed their faith in Caesars to store the data in a safe and secure manner. And as shown above, the criminal acts of third parties resulting in the Data Breach were foreseeable. Thus, as it relates to the securing of that information, the parties do not deal on equal terms; instead, Plaintiffs had no control over the process by which Caesars stored and maintained their PII. Both Nev. Rev. Stat. § 603A and the FTC Act (15 U.S.C. § 45) impose a special relationship between Caesars and Plaintiffs that requires Caesars to protect PII and adopt reasonable security procedures.

2. Plaintiffs Adequately Plead Breach of Duty Owed to Them.

Caesars next argues that even if a duty of care arose, Plaintiffs fail to allege any conduct that breached that duty. Mot. at 17-19. To the contrary, and despite Caesars' secrecy concerning the specific security flaws exploited in the Breach, the CAC details Caesars' inadequate information security.

First, Caesars made the business decision to aggregate information of tens of million individuals. CAC ¶ 3. Then, Caesars chose to keep Class Members' PII for years after the original hotel stays, much longer than was necessary to achieve the goal of processing the consumers' hotel room rentals. *Id.* ¶ 396. These facts demonstrate Caesars' failure to adhere to standard purging and data minimization processes. *Id.* ¶253 (FTC recommendations in this regard). Caesars should have deleted consumers' sensitive PII when it was no longer needed.

Second, Caesars "intentionally failed to encrypt the PII while it was stored on Caesars' server." CAC ¶ 430. No adequate data security program would permit any of these circumstances. *See id.* ¶ 253.

Third, a reasonable data security program would have monitored sensitive systems for suspicious activity like transfers of bulk data. An adequate system would have stopped the data exfiltration. Yet, Caesars allowed an intruder to download the PII for millions of customers five days after it supposedly noticed the suspicious activity. CAC ¶ 225. Instructive is *Smallman*:

> Plaintiffs allege that Defendant MGM breached their duty of care in their manner of collecting, maintaining, and controlling their customers' sensitive personal and financial information. (CAC ¶ 7). Specifically, Plaintiffs contend that Defendants breached this duty by retaining Plaintiffs PII for longer than necessary (Id. ¶¶ 7, 91), "fail[ing] to encrypt the PII stores on its server" (Id. ¶ 40), deviating from industry best practices as laid in the Federal Trade Commission and National Institute of Standards and Technology guidelines, (Id. ¶¶ 66–76), and otherwise "fail[ing] to adopt reasonable safeguard to protect Class members' PII (Id. ¶ 87)." At this stage in the pleading, Plaintiffs have sufficiently alleged that Defendants breached the duty of care owed to them.

638 F. Supp. 3d at 1188.

Caesars does not rely on any cases that include all of these allegations. *See* Mot. 17. Further, Caesars' argument that it is absolved of liability because its IT vendor gave the cybercriminal access to its servers is preposterous. Mot. 18. The IT vendor is part of Caesars' security apparatus. The vendor's ability to give the cybercriminal unfettered access to the unencrypted PII in Caesars' system without sufficient oversight—based on essentially a prank call—is a further breach of Caesars' duty.

3. The Economic Loss Doctrine Does Not Apply Because Plaintiffs Adequately Cognizable Non-Economic Damages.

Contrary to Caesars's argument (Mot. 18), the economic loss doctrine is inapplicable and does not bar recovery because (i) Plaintiffs allege non-economic damages, (ii) Caesars duty is based on statutory obligations, and (iii) a special relationship exists.

To determine whether the economic loss doctrine precludes claims, Nevada courts employ a two-step process: first, ascertain whether the loss is purely economic in nature; and second, ascertain whether the economic loss doctrine actually applies to a plaintiff's claims. See *Copper Sands Homeowners Ass'n, Inc. v. Copper Sands Realty, LLC*, 2012 WL 1044311, at *4 (D. Nev. Mar. 27, 2012). The doctrine is inapplicable where a plaintiff alleges both economic and non-economic losses including harm to plaintiff intangible property. *Lopez v. Javier Corral, D.C.*, 2010 WL 5541115, at *3-4 (Nev. Dec. 20, 2010) (finding economic loss doctrine inapplicable because plaintiff alleged non-economic damages including lost time and reputational harm).

Here, Plaintiffs have incurred non-economic harms such as loss of control over the use of their identity, loss of their time, risk of embarrassment, enlarged risk of identity theft, and invasion of their privacy in addition to their economic harms. CAC ¶¶ 18, 29, 39, 50, 60, 70, 81, 91, 101, 110, 120,

129, 139, 150, 161, 170, 179, 189, 200. In *MGM*, this Court rejected the argument that the economic loss doctrine barred plaintiffs' negligence claims with nearly identical allegations of harm because they were non-economic. 638 F. Supp. 3d 1175, 1188 (D. Nev. 2022).[7] The dissemination of Plaintiffs' PII here, as in *MGM*, has diminished Plaintiffs' control over their digital and physical identities. As such, the economic loss doctrine is inapplicable. *Accord Flores-Mendez v. Zoosk, Inc.*, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021) ("Plaintiffs allege their loss of time, risk of embarrassment, and enlarged risk of identity theft as harms and, so do not allege pure economic loss."); *Mehta v. Robinhood Fin. LLC*, 2021 WL 6882377, at *6 (N.D. Cal. May 6, 2021) (alleged harms derived from the "loss of control over their use of their identity" and right to privacy are non-economic).

If the Court gets to the second step (and it need not), Nevada courts have recognized that where a duty of care is premised on a statutory obligation, not a contractual promise, the economic loss doctrine does not apply. *See Lucatelli v. Texas De Brazil (Las Vegas) Corp.*, 2012 WL 1681394, *4 (D. Nev. May 11, 2012) (finding that because duty to pay overtime wages arose from statutory, not contractual, obligations the economic loss doctrine was inapplicable). As detailed above, Caesars had myriad statutory obligations requiring it to safeguard plaintiffs' private data. These duties and the harms resulting from their breach are outside the scope of the economic loss doctrine.

Finally, as detailed above, Caesars stood in a "special relationship" with Plaintiffs and the putative class qualifying for an exception to the economic loss doctrine, such as in professional negligence actions. See *Lopez*, 2010 WL 5541115, at *3-4 ("'courts have made exceptions [to the economic loss doctrine] to allow recovery in certain categories of cases, such as negligent misrepresentation and professional negligence actions'") (citation omitted).

4. Plaintiffs have also alleged plausible claims for *per se* negligence.

As part of their claim for negligence, Plaintiffs plead a viable *per se* negligence claim based on Caesars' violation of federal and state data security statutes. CAC ¶¶ 329-334. "A statutory violation

[7] Numerous courts recognize that in the data breach context, claims to recoup the value of lost time are not barred under the economic loss doctrine. See *Solara*, 613 F. Supp. 3d at 1296 (interpreting California law); *Stasi*, 501 F. Supp. 3d at 912-14 (same); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039-40 (N.D. Cal. 2019) (same); *Flores-Mendez v. Zoosk, Inc.*, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021) (same).

is negligence *per se* if the injured party belongs to the class of persons whom the statute was intended to protect, and the injury suffered is of the type the statute was intended to prevent." *Atkinson v. MGM Grand Hotel, Inc.*, 98 P.3d 678, 680 (Nev. 2004). Further, "liability under a negligence *per se* theory is in general a question of fact for the jury." *Anderson v. Baltrusaitis*, 944 P.2d 797, 799 (Nev. 1997) (citation omitted).

Here, Plaintiffs and class members belong to the class of persons whom the FTC Act, Nevada's data privacy law, and similar state statutes requiring reasonable data security measures seek to protect as they are consumers whose PII is possessed by Caesars. *See, e.g.*, Nev. Rev. Stat. § 603A.300 (defining "consumer"). And, the harm alleged is the type that the statutes were intended to prevent. Therefore, Plaintiffs have plausibly alleged *per se* negligence.

Caesar, relying on *Baton v. Ledger SAS*, 2024 WL 3447511 (N.D. Cal. July 16, 2024), argues that Plaintiffs cannot sustain their *per se* negligence claim based on violation of the FTC Act because the Act itself does not permit a private cause of action. Mot. at 16. That case is inapt as it was decided under California law, which does not permit negligence *per se* as a stand-alone cause of action. Moreover, Caesars ignores two other decisions which properly held that a violation of the FTC Act could support negligence *per se* as under California law as an evidentiary presumption in support of a negligence claim. *See Kirsten v. California Pizza Kitchen, Inc.*, 2022 WL 16894503, at *8 (C.D. Cal. July 29, 2022), reconsideration denied, 2022 WL 16894880 (C.D. Cal. Sept. 8, 2022) (denying motion to dismiss plaintiffs' negligence per se claim); *In re Ambry Genetics*, 567 F. Supp. 3d at 1142–43 (same).

Caesars also ignores numerous other federal district court decisions that have upheld negligence *per se* pleadings in data breach cases solely on the basis of FTC Act. *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d at 1327 ("The Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect. […] The Defendants' motion to dismiss the negligence per se claim should be denied."); *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 684 (D.S.C. 2021) (same under South Carolina law); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407–08 (E.D. Va. 2020) (same under New York law); *First Choice Fed. Credit Union v. Wendy's Co.*, 2017 WL

9487086, at *4 (W.D. Pa. Feb. 13, 2017), report and recommendation adopted, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760–61 (C.D. Ill. 2020) ("[T]he FTC Act can serve as the basis of a negligence per se claim."); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 482 (D. Md. 2020). Similarly, here, violation of the FTC Act can serve as a basis for Plaintiffs' negligence per se claim.

Second, contrary to Defendant's argument, Plaintiffs and Class Members are in the class of individuals that the Nevada's data protection statute (Nev. Rev. Stat. § 603A.210) was intended to protect even if they are not Nevada residents. The statute states: "[a] data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." *Id.* Rather than creating one standard for the PII of Nevada residents and another for non-Nevada residents in Caesars records, the statute requires reasonable security measures for all PII in Caesars' records, including that of all Plaintiffs.

Third, Defendant argues that Plaintiffs cannot "rest their negligence per se on 'similar state statutes.'" Mot. at 16. This is wrong. Plaintiffs can assert claims in negligence per se on the basis of various states' data protection statutes (CAC ¶330-332), where the language of these statutes does not expressly preclude private rights of action. *See In re Equifax, Inc.*, 362 F. Supp. 3d at 1341 (declining to dismiss claims under state data privacy statutes because "Defendants have not identified any authority construing this language [contained in the data breach statutes] as precluding private rights of action."); *Perdue*, 455 F. Supp. 3d at 767–68 ("Absent any authority construing this ambiguity to exclude private rights of action, the [Kansas PCI] claims should not be dismissed."); *In re Target Corp.*, 66 F. Supp. 3d at 1170.

Finally, to the extent Defendant argues that some of the claims under state data protection statutes are not viable, that is a merits argument, which ought to be addressed at a later stage.

C. Plaintiffs Adequately Plead an Implied Contract Claim.

Caesars does not challenge that an implied contract exists, only that Plaintiffs fail to identify "any specific promise Caesars made," and any term that was breached, and that Plaintiffs fail to allege cognizable injuries. Mot. at 19-21. The Court in *MGM* rejected these same arguments, finding: "[It is

difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of ... sensitive personal information would not imply the recipient's assent to protect [the] information sufficiently.'" *MGM*, 638 F. Supp. 3d at 1195 (collecting cases), citing *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *9.

Under Nevada law, "whether a contract exists is [a question] of fact." *Certified Fire Prot. Inc. v. Precision Constr.*, 283 P.3d 250, 255 (2012). Thus, whether an implied contract exists here is not a question appropriately resolved by a Rule 12(b)(6) motion.

Nevertheless, Plaintiffs have alleged facts sufficient to demonstrate that an implied contract exists. Just as in *MGM*, Caesars solicited the Plaintiffs to provide Plaintiffs' PII during the reservation and check-in process, when signing up for Caesars Rewards, and when gambling. CAC ¶¶ 4-5, 14, 25, 36, 46, 56, 66, 78, 88, 98, 210-216, 345-350. Plaintiffs provided their PII with the mutual understanding and expectation that Caesars would implement reasonable and adequate data security measures and that Caesars' data security practices complied with relevant laws, regulations, and industry standards. CAC ¶ 214. This mutual understanding is based in part on Caesars' privacy policy which stated that Caesars is "committed to respecting your data privacy," and that it "maintain[s] physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control. CAC ¶ 215. Many courts have found that plaintiffs adequately pled implied contract claims based on similar facts in data breach cases. *See, e.g., Solara*, 613 F. Supp. 3d at 1297 (denying motion to dismiss an implied contract claim based on similar allegations); *Marriott*, 440 F. Supp. 3d at 486; *Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713, at *11 (S.D.N.Y. May 7, 2019) (collecting cases); *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015), *aff'd sub nom. Enslin v. Coca-Cola Co.*, 739 F. App'x 91 (3d Cir. 2018) (concluding defendants "implicitly promised to safeguard his PII"); *In re Marriott*, 440 F. Supp. 3d at 486 (refusing to dismiss implied-in-fact contract count).

The cases cited by Caesars are inapposite. Unlike *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717-18 (8th Cir. 2017), where plaintiffs did "not identify a single 'applicable law and regulation'" that defendant breached, the CAC identifies numerous laws, regulations, and industry standard practices that Caesars disregarded. Caesars' argument that there was no breach of the implied contract parallels

its argument that there was no negligence. Caesars failures to properly protect its customers' information are set out in detail in the CAC.

As to cognizable damages for breach of implied contract, "[t]he dissemination of one's personal information can satisfy the damages element of a breach of contract claim." *Solara*, 613 F. Supp. 3d at 1297. Plaintiffs have pled that harm in detail. *See* Sections III.A.1.a & A.4, *supra.*

D. Plaintiffs Adequately Plead a Claim in Unjust Enrichment.

Caesars attacks Plaintiffs' unjust enrichment claim, plead in the alternative, on two grounds. First, Caesars claims Plaintiffs cannot show they lack an adequate remedy at law as required by *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 845 (9th Cir. 2020)[8]. Mot at 21. Caesars is wrong.

The CAC alleges that Plaintiff have no adequate remedy at law because Caesars retains their PII while exposing the PII to a risk of future data breaches while in Caesars' possession. CAC ¶ 366. Plaintiffs allege facts establishing that they are entitled to injunctive relief (CAC ¶¶ 304-306, 355) and request such injunctive relief across all applicable causes of action. *See* CAC Request for Relief (d). Plaintiffs seek an injunction "requiring Caesars to: (i) strengthen its data security systems and procedures; (ii) submit to future annual audits of those systems by a Court appointed independent auditor; and (iv) delete PII that Caesars no longer needs for processing services previously provided to Class Members." *Id.* This injunctive relief can sustain a claim for unjust enrichment. *Cf. MGM*, 638 F. Supp. 3d at 1198 (dismissing plaintiffs' unjust enrichment claim because plaintiffs did not seek injunctive relief, but granting leave to amend).

Second, Caesars asserts that Plaintiffs failed to plead facts showing that Caesars received a "benefit" that was "unjustly" retained. Mot at 22. Caesars posits that the "monetary consideration" it

[8] In any event, *Sonner* is not controlling here. First, it was decided under California, not Nevada law. *Sonner*, 971 F.3d at 844. Second, in *Sonner*, "the plaintiff sought leave to dismiss her CLRA claim and add a claim for restitution less than two months before the trial" to avoid a jury trial. *Krause-Pettai v. Unilever U.S., Inc.*, 2021 WL 1597931, at *4 (S.D. Cal. Apr. 23, 2021). No such gamesmanship is present here as the count has been plead in the alternative under FRCP 8(d)(2) and the case is at the pleading stage. Third, the *Sonner* challenge is premature because, at this stage, Plaintiffs cannot "'quantify [their] actual damages for future harm' with any certainty[.]" *Rothman v. Equinox Holdings, Inc.*, 2021 WL 1627490, at *12 (C.D. Cal. Apr. 27, 2021) (quoting *Integrity MessageBoards.com v. Facebook, Inc.*, No. 18-CV-05286-PJH, 2020 WL 6544411, at *7 (N.D. Cal. Nov. 6, 2020)).

received is insufficient to show a benefit. *Id.* But this argument ignores both that Caesars received the money, *and Plaintiffs' PII*, and the growing body of law that accepts that:

> the failure to secure a party's data can give rise to an unjust enrichment claim where a defendant accepts the benefits accompanying plaintiff's data and does so at the plaintiff's expense by not implementing adequate safeguards, thereby making it 'inequitable and unconscionable' to permit defendant to retain the benefit of the data … while leaving the plaintiff party to live with the consequences.

In re Capital One Consumer Data Security Breach Litigation, 488 F. Supp. 3d 374, 412 (E.D. Virginia 2020); *Sackin v. TransPerfect Glob.*, Inc., 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017) ("it would be inequitable and unconscionable to allow TransPerfect to retain the money it saved by shirking data-security, while leaving Plaintiffs to suffer the consequences").

Plaintiffs allege they did not receive equal value in exchange for what they paid. The money Plaintiffs paid for hotel rooms was for, inter alia, Caesars' services "as well as adequate safeguarding of [Plaintiffs'] PII." CAC ¶358. Caesars failed to spend the money that was intended to be used for reasonable data security for this purpose, but kept all of the funds. CAC ¶360-361.

Plaintiffs have pled that Caesars was enriched by the receipt of Plaintiffs' PII, on top of monetary revenue Caesars uses this PII "for a variety of profit-generating purposes beyond simply providing its services," including "to generate future stays from consumers and derive future revenues and profit." CAC ¶359. Plaintiffs also allege that the PII has independent and significant monetary value. CAC ¶¶ 280, 283. In other words, Caesars has been enriched because it provided less than what it was paid for and profited from the retention and use of Plaintiffs' PII.

E. Plaintiffs' Consumer Protection Claims are Pled with Sufficient Particularity.

Caesars broadly pronounces that Plaintiffs' statutory claims universally fail as insufficiently pleaded under FRCP 9(b), dropping a string cite to cases that applied a heightened pleading standard to unspecified claims under state consumer protection statutes. Mot. at 22. As an initial matter, Rule 9(b) heightened pleading does not apply because Plaintiffs do not allege *intentional* fraud by Caesars, instead alleging negligence-based or reckless conduct, and a failure to disclose material information about Caesars security status. Caesars's tactic of arguing in the aggregate elides important distinctions between the statutes, their varying pleading requirements, and even ignores entire theories of liability.

Caesars failed to provide the Court with the applicable legal standards, explain why Rule 9(b) applies to each claim pled, or explain why Plaintiffs' allegations fall short.

Even if Caesars had adequately raised a Rule 9(b) challenge, Plaintiffs allege each of the facts that Caesars claims are missing. The CAC describes the specific data security practices Caesars neglected, explains what Caesars should have done, describes how Caesars knew it was a prime target for hackers, and explains that Caesars should have disclosed its deficient practices to rewards members. *Compare* Mot. at 26 (listing information Plaintiffs should have pleaded) *with* CAC ¶¶ 252-68 (detailing how Caesars neglected best practices for data security), ¶¶ 243-51 (Caesars knew it was at risk of a cyberattack), ¶¶ 239-42 (Caesars failed to disclose its deficient management of PII).

Faced with almost identical allegations, the court in *MGM* found that the plaintiffs' allegations met the requirements of Rule 9(b) explaining that (1) "Plaintiffs allege that Defendant [] knew its data security practices were deficient and that the hotel industry is a frequent target of sophisticated cyberattacks"; (2) "[d]espite this knowledge, Plaintiffs allege that Defendant [] declined to disclose any facts regarding its cybersecurity"; and that (3) "Plaintiffs allege that Defendant [] failed to implement reasonable security measures to protect its servers, including encrypting consumer's PII, . . . retained Plaintiffs PII for longer than necessary, . . . and that Plaintiffs were damaged as a result of the Data Breach." *See MGM*, 638 F. Supp. 3d at 1199–20. Like in *MGM*, "Plaintiffs sufficiently allege that Defendant MGM's failure to disclose its data security deficiency or vulnerability to Plaintiffs constitutes a 'knowing' omission." *MGM*, 638 F. Supp. 3d at 1200 (quoting *Poole v. Nevada Auto Dealership Invs., LLC*, 449 P.3d 479, 483 (Nev. App. 2019)). Thus, although the particularity pleading requirement is relaxed where, as here, the facts concerning fraudulent conduct are exclusively in the hands of a defendant, *see Neubronner v. Milken*, 6 F.3d 666, 672 (9th Cir. 1993), Plaintiffs' claims are more than sufficiently pled.

Plaintiffs also adequately allege reliance. The Complaint states that they "relied on Caesars' policies and promises to implement sufficient measures to protect [their] PII and privacy rights," and that had they "been informed that Caesars had insufficient data security measures to protect [their] PII, [they] would not have enrolled with Caesars Rewards or have gamed at Caesars as frequently or at all." CAC ¶¶ 21, 32, 42, 52, 62, 73, 83, 93, 103, 112, 123, 131, 141, 153, 163, 172, 181, 193, 202; *see*

also id. ¶ 217 ("Plaintiffs and Class Members relied on the sophistication of Caesars to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information."). Caesars contends that Plaintiffs do not allege they actually read the policies, but Plaintiffs need only establish that "had the omitted information been disclosed, the plaintiff would have been aware of it and behaved differently." *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *35 (N.D. Cal. May 27, 2016). This is enough to plead "actual reliance" based on a fraudulent omission. *See id.* at *36.

Lastly, Plaintiffs plausibly allege that Caesars knew its security policies were deficient and that it was particularly vulnerable to cyberattack, but failed to implement reasonable security measures. *See* CAC ¶¶ 252-68 (Caesars neglected best practices for data security), ¶¶ 243-51 (Caesars knew it was at risk of a cyberattack), ¶¶ 239-42 (Caesars failed to disclose its deficient management of PII). Caesars is wrong that Plaintiffs do not allege "any specific failure" relating to Caesars' use of "reasonable security procedures." Mot. at 26. For example, Plaintiffs' allegations include that Caesars held Plaintiffs' "unencrypted PP" on its server, CAC ¶ 213, which Scattered Spider was able to download from the member database, CAC ¶ 224, and that data "remains unencrypted and available for unauthorized third parties to access and abuse," CAC ¶¶ 18, 29, 39, 50, 60, 70, 81, 91, 101, 110, 120, 129, 139, 150, 161, 170, 179, 189, 200, 430. Plaintiffs further allege that Caesars retained customers' PII "much longer than was necessary to achieve [its] goals." CAC ¶ 396; and that it was slow to identify and act on suspicious activity; CAC ¶ 225("Caesars identified the suspicious activity on August 18, 2023, yet Scattered Spider downloaded the unencrypted PII five days later.") These specific failures are well pleaded in the Complaint. *See In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1219 (S.D. Fla. 2022) (holding that plaintiffs sufficiently alleged a claim under the CRA by alleging that their "PII [was] maintained and/or exchanged in unencrypted email accounts, in violation of industry best practice"); *MGM*, 638 F. Supp. 3d at 1188, 1200, 1205.

F. Plaintiffs' Notification Claims Allege Cognizable and Incremental Harm.

Caesar argues that Plaintiffs' claims based on timely disclosure statutes fail to allege actual harm caused by the delay. This is incorrect. Plaintiffs allege that Caesars' delay in notifying states' attorneys general, and sending individual notices, "exacerbated the harm to Class Members by

preventing them from taking steps to mitigate Caesars failures and trying to protect themselves." CAC ¶ 230. Plaintiffs also allege that "Caesars has not, to this date, disclosed: how many of its loyalty rewards program members were affected by the Data Breach; what information was taken; how the cybercriminals were able to exploit vulnerabilities in Caesars' data systems; the identity of Caesars' outside IT vendor; the identity of the hacking group responsible for the Data Breach; or what steps Caesars has taken to ensure that such an attack does not happen." CAC ¶ 232. Absent this information, Class Members still cannot fully understand or mitigate the harm from the Breach. CAC ¶ 233.

Plaintiffs' allegations encompass exactly the type of harm contemplated by the timely disclosure statutes in California, Illinois, and Virginia. For example, under the California Consumer Record Act, courts have found incremental harm adequately pled "when plaintiffs plausibly alleged that they could not take mitigation steps based upon delay." *See Solara*, 613 F. Supp. 3d at 1300 (citing *In re Yahoo! Inc.*, 2017 WL 3727318). Similarly, under both the California and Illinois statutes, where plaintiffs allege "post-remedial actions and harm from the Data Breach," courts find it "plausible to conclude that Defendants' more timely disclosure would have prevented additional incremental injury." *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 590 (N.D. Ill. 2022). And in Virginia, it is sufficient to allege "additional monitoring costs that [the plaintiff] would not have otherwise taken" to fall within the scope of the statute. *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d at 416–17.

G. Plaintiffs' Statutory Claims Are Adequately Pled.

1. Plaintiffs Adequately Plead the Nevada Consumer Fraud Act Claim.

Plaintiffs alleged violations of two subsections of Nev. Rev. Stat. § 598 ("NDTPA"). First, Nev. Rev. Stat. § 598.0923(2) provides that a deceptive trade practice includes knowingly failing to "disclose a material fact in connection with the sale or lease of goods or services" in the course of one's business or occupation. Relying on nongermane cases, Caesars argues that Plaintiffs do not have a claim under § 598.0923(2) because Caesars did not have a duty to disclose in the absence of a special relationship between plaintiffs. Mot. at 43, citing *Soffer v. Five Mile Capital Partners, LLC*, 2013 WL 638832, at *10 (D. Nev. Feb. 19, 2013) and *Taddeo v. Taddeo*, 2011 WL 4074433, at *6 n.3 (D. Nev. Sept. 13, 2011). However, as other Courts have recognized, those cases apply to *common law fraud* claims

rather than statutory consumer fraud claims. *See, e.g., MGM,* 638 F. Supp. 3d at 1199. But "[s]tatutory offenses that sound in fraud are separate and distinct from common law fraud." *Id.* (citing *Leigh-Pink v. Rio Props, LLC*, 512 P.3d 322, 328 (Nev. 2022)) (internal citations omitted). Regardless of the defect in Caesars' authority, Caesars stood in a special relationship to Plaintiffs because the parties did not stand on equal footing. See Section II.B.1, *supra.*

Second, Nev. Rev. Stat. § 598.0923(3) creates liability for persons who "knowingly ... violate[] a state or federal statute or regulation relating to the sale or lease of ... services." *Id.* Plaintiffs outlined violations of state and federal statutes, namely Nev. Rev. Stat. § 598.0923(2) (requiring disclosure of material facts), Nev. Rev. Stat. § 603A.210(1) (requiring "reasonable security measures"), and 15 U.S.C. § 45 ("FTC Act") (requiring reasonable data security)—as well as violations of California, Illinois, Indiana, Minnesota, New York, Pennsylvania, Texas consumer protection and/or data security statutes. CAC ¶¶ 373-375. Therefore, if the Court finds that any of Plaintiffs' state law causes of action survive, Plaintiffs' Nev. Rev. Stat. § 598.0923(3) claim must survive, too.

Caesars argues that Plaintiffs cannot state a claim under Nev. Rev. Stat. § 598.0923(3) because Nev. Rev. Stat. § 603A.210(1) only applies to residents of Nevada, and no plaintiffs are residents of Nevada. However, Plaintiffs assert § 603A as a predicate violation for a § 598.0923(3) violation, not as a separate cause of action. Section 603A provides that "[a] data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." Nev. Rev. Stat. § 603A.210(1). Caesars is a data collector that maintains records of in-state residents. Caesars violated § 603A.210(1), thus violating § 598.0923(3).

Lastly, Caesars argues that Plaintiffs have failed to allege that Caesars violated the FTC Act. But the FTC Act "treats the failure to employ reasonable data security safeguards as an unfair act or practice." CAC ¶ 256; *see In re Equifax.*, 362 F. Supp. 3d 1295 at 1327-28. The CAC is replete with allegations that Caesars knew that its security practices were deficient, was fully aware of its obligations to use reasonable and adequate measures to protect Plaintiffs' PII, and simply failed to do so. *See, e.g.*, CAC ¶¶ 252-260; 369-381.

2. Plaintiff Complied With the DTPA'S Pre-Suit Notice Requirement.

Caesars asserts that Plaintiff Huddleston failed to meet the pre-suit notice requirement for his Texas Deceptive Practices Act ("DTPA") claim. But Caesars is wrong. CAC ¶¶ 560, 562. On June 28, 2024, and July 29, 2024, Plaintiff's counsel sent letters to Caesars' counsel detailing Plaintiff's complaint and providing notice of the impending lawsuit. *See* Ex. A, Ltr. from A. Keller (June 28, 2024); Ex. B, Ltr. from S. Soneji (July 29, 2024). The letter summarized what was publicly known about the data breach, and that "Caesars' conduct remains un-remedied in violation with numerous consumer protection statutes," including the DTPA. *Id.* at 2–3. The letter explicitly noted that it served as "additional notice" of the Plaintiffs' demands. *Id.*

More critically, Caesars' requested remedy of abatement would serve no purpose. Under the DTPA, abatement is only required "if, after hearing, the trial court finds that a party entitled to notice did not receive it." *In re Liberty Mut. Fire Ins. Co.*, 2010 WL 1655492, at *3 (Tex. App. Apr. 27, 2010) (citing Tex. Bus. & Com. Code Ann. § 17.505(d)). After that, "abatement continues until the 60th day after that written notice is served." *Id.* (citing Tex. Bus. & Com. Code Ann. § 17.505(e)). Here, Caesars received Mr. Huddleston's complaint nearly three months ago, and the 60-day window for abatement under Texas law has already passed. And although Plaintiff's notice was sent approximately 30 days before the Consolidated Complaint—as opposed to 60—abatement would not fulfill the spirit of the rule, which is "to discourage litigation and encourage settlement of consumer complaints." *Richardson v. Foster & Sear, L.L.P.*, 257 S.W.3d 782, 784 (Tex. App. 2008) Caesars was served with numerous prior complaints in connection with the Data Breach, *see* CAC ¶ 560, and thus, earlier complaints provided Caesars with written notice of the factual bases of Plaintiff's cause of action well in advance of the 60-day period. *Cf Richardson*, 257 S.W.3d at 786(finding that a notice "fulfils the purpose of the notice requirement" where it is sufficient "to allow [a defendant] to determine whether to settle . . . or undertake the cost and risk of litigation").

Nor can Caesars show any harm from the alleged technical violation of the timing requirement. Courts excuse delay where defendants are "not harmed by the [plaintiff's] alleged technical violation" of the timing requirement. *Star Houston, Inc. v. Kundak*, 843 S.W.2d 294, 297 (Tex. App. 1992); *see also Star-Tel, Inc. v. Nacogdoches Telecomms., Inc.*, 755 S.W.2d 146, 149 (Tex. App. 1988).

3. Plaintiffs Adequately Plead the California UCL and CLRA Claims

a. Plaintiffs Have Established Standing under the UCL and CLRA

Caesars asserts that Plaintiffs lack standing under their California statutory claims because they have not established that they "lost money or property", or "economic injury." Mot. at 44-45. Not so. Plaintiffs allege the loss of value of their breached PII. CAC ¶¶ 277-285, ¶410. Plaintiffs also suffered benefit of the bargain damages, including overpayment for hotel rooms and for Caesars' services. CAC ¶¶ 21, 32, 42, 287-291, 407. The complaint also pleads that "[h]ad Plaintiffs known the truth about Caesars' deficient data security practices, they would not have stayed at Caesars properties or would have paid less than they did for their rooms." *Id.* ¶ 290. Plaintiffs also allege out-of-pocket costs in mitigation efforts, including for lost time spent monitoring their accounts for fraud and identity theft; time spent managing spam calls, emails, and texts; late fees imposed because of fraudulent credit card charges, and purchasing identity protection services. CAC ¶¶ 16, 17, 20, 28, 30, 31, 38, 40, 41, 407, 426, 272. Caesars' notice to consumers recommended customers enroll in credit monitoring and identity protection services, monitor their accounts; place fraud alerts or credit freezes with their credit reporting agencies; and to contact the FTC.[9] While Caesars did provide minimal credit monitoring, Plaintiffs found that more was necessary to protect themselves.

These facts establish standing under the UCL and the CLRA. *See, e.g., MGM,* 638 F. Supp. 3d at 1202 (upholding UCL and CLRA claims, and recognizing damages in the form of overinflated cost of hotel rooms, loss of value of PII, increased risk of identity fraud, lost time); *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1219-220 (C.D. Cal. 2017) (allegation by plaintiffs that they would not have purchased or would have paid less for product if defendant had properly disclosed its consumer data collection and disclosure practices); *In re Anthem Data Breach Litig.,* 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) ("benefit of the bargain damages represent economic injury for purposes of the UCL."); *In re Yahoo! Inc.*, 2017 WL 3727318, at *14 ("allegations that [plaintiffs'] PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the

[9] Caesars 2023 Notice of Data Breach template, https://www.mass.gov/doc/assigned-data-breach-number-30726-caesars-entertainment-inc/download, last accessed Oct. 12, 2024.

dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury arising from [] Data Breaches."); *Calhoun*, 526 F. Supp. 3d at 636 (loss of personal data constitutes economic injury for standing under the UCL); *Levitt v. Yelp! Inc.*, 2011 WL 13153230, at *7 (N.D. Cal. Mar. 22, 2011) (quoting *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 891 n.15 (Cal. Jan. 27, 2011)).

Caesars' citations to the contrary are distinguishable from the situation here. *Gardiner,* for instance, concerned the breach of expired and invalid credit card numbers—that is, valueless PII—unlike the social security numbers, driver's license numbers, and other valuable information at issue here. *Gardiner v. Walmart, Inc.,* 2021 WL 4992539, at *3-4 (N.D. Cal. July 28, 2021). Moreover, as described above, the lawsuit here is based on much more than "mere allegations of worry;" there is a real threat of increased risk of fraud and identity theft. *Compare with Kuhns*, 868 F.3d at 718.

b. Plaintiffs' injuries were caused by the Data Breach.

Caesars claims that Plaintiffs have failed to allege actual reliance on any representation or omission. But reliance is only required for claims under the fraud prong of the UCL. *See In re Tobacco II Cases*, 46 Cal. 4th 298, 325 n.17 (2009) ("There are doubtless many types of unfair business practices in which the concept of reliance, as discussed here, has no application.") Moreover, as Defendant's own citation makes clear, under California law, "at the motion to dismiss stage, actual reliance ... is inferred from the misrepresentation of a material fact." *Moore v. Mars Petcare US, Inc.*, 966 F.3d 1007, 1021 (9th Cir. 2020). Indeed, to allege reliance on a misrepresentation, "a plaintiff "only need[ ] establish it to be plausible that a 'reasonable man would attach importance to [the] existence or nonexistence [of the misrepresentation] in determining his choice of action in the transaction in question.'" *Id.* (internal citations omitted); *see also Broomfield v. Craft Brew All., Inc.*, 2017 WL 3838453, at *5 (N.D. Cal. Sept. 1, 2017), *on reconsideration in part*, 2017 WL 5665654 (N.D. Cal. Nov. 27, 2017), Plaintiffs must allege facts to show the alleged misrepresentations are 'likely to deceive' a reasonable consumer). To allege reliance on an omission, Plaintiffs need only establish that "had the omitted information been disclosed, the plaintiff would have been aware of it and behaved differently." *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at * 35 (N.D. Cal. May 27, 2016).

Plaintiffs describe in detail the specific data security practices Caesars neglected, explains what Caesars should have done, describes how Caesars knew it was a prime target for hackers, and that it should have disclosed its deficient practices to rewards members. CAC ¶¶394, 395, 396, 398-404. Caesars also misrepresented that it would protect class members PII and would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' PII. CAC ¶¶ 404. Plaintiffs also allege that they would not have stayed at, gambled at, or would have paid less for Caesars' properties and services had they known the truth about Caesars deficient data security. CAC ¶¶ 21, 32, 42, 290. That is more than sufficient at this stage.

c. Caesars' Other Challenges to the UCL Also Fail.

Caesars asserts several other bases for dismissal which should be rejected. Caesars states that Plaintiffs lack a viable UCL claim because they are not entitled to equitable relief under the UCL when they have "adequate legal remedies" under their other claims. Mot. at 33 citing *Sonner ,* 971 F.3d 834. As discussed above, *Sonner* is inapt here. See Section III.D, *supra*. Moreover, the ongoing, prospective nature of the UCL claim and that some aspect of the injury pled might not have an adequate remedy at law have been held to distinguish *Sonner* and preclude dismissal at this early stage *MGM,* 638 F. Supp. 3d at 1200; *Stewart v. Kodiak Cakes, LLC*, 2021 WL 1698695, at *35 (S.D. Cal. Apr. 29, 2021).

Caesars next claims that Plaintiffs failed to show any unlawful, unfair, or fraudulent conduct. Mot. at 47-48. Caesars' claims that Plaintiffs fail to state violations of the CCRA, CLRA and FTC Act is without merit, as addressed in Section III.G.3.d (CLRA), and section III.B.4 (Nevada CFA, addressing violations of the FTC Act under California law). Also lacking merit is Caesars' argument that Plaintiffs cannot allege a claim under the "fraud" prong of the UCL because no reasonable consumer could be deceived since Caesars Privacy Policy includes a disclaimer of security. Mot. at 34. Such a determination is inappropriate at this stage as "[c]ourts have recognized that the deceptive nature of a business practice under California's consumer protection statutes is usually a question of fact that is inappropriate for decision on demurrer or a motion to dismiss." *Broomfield*, 2017 WL 3838453, at *5. But Caesars also takes the text out of context. The supposed one-sentence disclaimer is "that [Caesars] cannot guarantee or warrant the security of any information you transmit on or

through a website or mobile app, and you do so at your own risk," but the remainder of the paragraph states:

> We maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control. With regard to information that you transfer to us through one of our websites or mobile apps, please be aware that no data transmission over the Internet or a wireless network can be guaranteed to be 100% secure.

CAC ¶239. Plaintiffs do not allege that their information was intercepted during transfer over a wireless network, but that it was intercepted from Caesars' systems when it was under Caesars' possession and control because of its inadequate safeguards. Lastly, Defendant ignores that Plaintiffs' allegations are not limited to the misrepresentations in Caesars' Privacy Policy, but concern far-ranging misrepresentations and omissions. CAC ¶¶ 394-405.

Caesars states that Plaintiffs' have failed to state a claim for unfair practices because they "do not allege why Caesars' purportedly unfair practices . . . amount to "unethical, oppressive, [and/or] substantially injurious" conduct." But "[n]one of the [California courts'] three tests for unfairness require plaintiffs to plead that defendants acted in an immoral, unethical, oppressive, or unscrupulous manner." *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d at 990 (finding a claim for unfairness because defendants' inadequate security violated California's public policy of protecting consumer data). Rather, it is sufficient to demonstrate that defendants' conduct violated an established California public policy. See *id*; *MGM*, 638 F. Supp. 3d at 1203.

Here, Plaintiffs have properly alleged that Caesars knowingly failed to implement reasonable security standards in violation of the data protection policy of specific California statutory provisions, subjecting Plaintiffs to substantial injury. CAC ¶¶ 386-390. Courts have consistently upheld such claims. *See MGM*, 638 F. Supp. 3d at 1203; *In re Yahoo! Inc.*, 2017 WL 3727318, at *24; *In re Anthem*, 162 F. Supp. 3d at 990; *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1227 (N.D. Cal. 2014).

d. Plaintiffs Adequately Plead Their CLRA Claim.

Caesars devotes four lines to dismissing the CLRA claim, stating it should be dismissed for the same reasons as the UCL claim. This includes that Plaintiffs have failed to allege reliance. Mot. at 32-33. As discussed above, such a determination is not appropriate at this stage. See III.G.3.c, *supra.*

Caesars also claims that Plaintiffs have failed to plead that Caesars engaged in unfair methods

of competition or unfair or deceptive acts or practices in a transaction intended to result in the sale of goods or services to a consumer. Mot. at 35. But this ignores the CAC allegations that Caesars omitted and concealed facts constituting unfair methods of competition or unfair or deceptive acts or practices, CAC ¶ 419, while engaged in in a transaction, *id.* ¶¶ 418, 424, intended to result in the sales of services, id. ¶¶ 419, 420, to consumers, *id.* ¶ 418. These core factual allegations support the CLRA claim.

4. Plaintiffs Adequately Plead Their Pennsylvania Claim.

Caesars next argues that Plaintiffs Smith and Katz's claims under the Pennsylvania Unfair Trade Practice and Consumer Protection Law ("UTPCPL") should be dismissed for failure to establish ascertainable loss in the form of "an actual loss of money or property." *Benner v. Bank of America, N.A.*, 917 F. Supp. 2d 338, 359 (E.D. Pa. 2013). Plaintiffs satisfied this requirement.

First, Plaintiff Katz alleged that he has "experienced numerous fraudulent transactions made on his credit card since the Data Breach." CAC ¶ 180. At the motion to dismiss stage, that is more than sufficient to show actual loss of money. Second, Plaintiffs identified specific property in the form of the lost value of their PII, "which serves as [a] form of lost property" under the UTPCPL. *Opris v. Sincera Reprod. Med.*, No. CV 21-3072, 2022 WL 1639417, at *13 (E.D. Pa. May 24, 2022); *Benner*, 917 F. Supp. 2d at 359 ("A plaintiff must be able to point to money or property that he would have had but for the defendant's fraudulent actions"). Plaintiffs alleged that they "suffered a 'loss of value of PII.'" CAC ¶ 276, 280-281; *see also id.* ¶¶ 170, 179, 276–85.

Plaintiffs Smith and Katz also plead facts to support justifiable reliance. "[A] plaintiff who asserts a UTPCPL claim that is based on a defendant's material omission may be entitled to a reasonable inference of reliance." *Cave v. Saxon Mortg. Servs., Inc.*, 2013 WL 460082, at *1 (E.D. Pa. Feb. 6, 2013) (citation omitted). Here, where Plaintiffs both allege that had they "been informed that Caesars had insufficient data security measures to protect [their] PII, [they] would not have enrolled with Caesars," it is reasonable to infer that Plaintiffs relied on Caesars' omissions. CAC ¶¶ 172, 181. In other words, Plaintiffs relied on Caesars to "compl[y] with industry requirements and standards," and therefore "were not in a position to know of the existence of any defects" in Caesars' security systems. *See Wilson v. Parisi*, 549 F. Supp. 2d 637, 668 (M.D. Pa. 2008).

In *In re Marriott*, the court concluded that plaintiffs' substantially similar allegations satisfied the Maryland Consumer Protection Act ("MCPA"), which involves an analogous presumption of reliance where omissions are material. *See In re Marriott*, 440 F. Supp. 3d at 489–90; *Tait v. BSH Home Appliances Corp.*, 289 F.R.D. 466, 484 (C.D. Cal. 2012) (noting that "a defendant's omission can be presumed by the materiality of the omitted fact"). There, the court held that plaintiffs sufficiently alleged reliance on defendants' material omissions because plaintiffs alleged that "Marriott's omissions would have been important to a significant number of consumers, that Plaintiffs relied on the omissions, and that Plaintiffs would not have paid Marriott for goods and services or would have paid less for such goods and services if it had known the truth about Marriott's alleged omissions." *In re Marriott*, 440 F. Supp. 3d at 489 (internal quotations omitted). Specifically, the court explained that "it [was] substantially likely that the consumer would not have made the choice in question had the commercial entity disclosed the omitted information." *Id.* at 489-90.

The same is true here. Plaintiffs alleged that Caesars' Privacy Policy "contained material omissions because it failed to disclose that Caesars' data security practices had significant shortfalls regarding its data systems that held consumers' PII," CAC ¶¶ 241, 538, that Plaintiffs "relied on Caesars' policies and promises to implement sufficient measures to protect [their] PII and privacy rights," CAC ¶¶ 172, 181, and that had Plaintiffs "would not have enrolled with Caesars Rewards or have gamed or stayed at Caesars as frequently or at all," *id.*, if they "had known the truth about Marriott's alleged omissions," *In re Marriott*, 440 F. Supp. 3d at 489. These allegations are enough to satisfy the UTPCPL's standard and establish an inference of reliance.

5. Plaintiffs Adequately Plead Their Virginia Claim.

Caesars makes only a token effort at dismissing Plaintiff Lackey's Virginia Consumer Protection Act ("VCPA") claim. In just over 10 lines, Caesars merely reincorporates its generalized arguments about the particularity of the pleading and states without elaboration that Plaintiff Lackey fails to plead facts demonstrating "actual damages." Mot. at 36-37.

Courts have routinely found that "actual damages" under the Virginia Consumer Protection Act are "expansive." *See e.g.*, *Attias v. CareFirst, Inc.*, 518 F. Supp. 3d 43, 56 (D.D.C. 2021); *Barnette v. Brook Rd., Inc.*, 429 F. Supp. 2d 741, 751 (E.D. Va. 2006) (finding that the VCPA authorizes recovery

for emotional distress); *In re Gen. Motors LLC Ignition Switch Litig.*, 339 F. Supp. 3d 262, 327, 332 (S.D.N.Y. 2018) (concluding that Virginia permits recovery for "lost free or personal time" stemming from consumer protection violations); *Wingate v. Insight Health Corp.*, 2013 WL 9564175 at *8 (Va. Cir. Ct. 2013) (noting that "'actual damages' as used in the VCPA is not limited to out-of-pocket pecuniary losses"). Here, Plaintiff Lackey expressly pleads that he is entitled to actual damages.

To start, Plaintiff Lackey pleads the loss of value of his PII. *See* CAC ¶¶ 200, 276–85. Courts have held that "allegations that [plaintiffs'] PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury arising from the Data Breaches." *In re Yahoo! Inc.*, 2017 WL 3727318, at *14. Second, Plaintiff Lackey alleged that he suffered benefit of the bargain damages, *see* CAC ¶¶ 200, 286–94, which he pleads with sufficient factual allegations about his "expectations for data security and the contours of the parties' bargain." *MGM*, 638 F. Supp. 3d at 1190. And third, Plaintiff Lackey alleged that he made significant mitigation efforts after the Data Breach, including but not limited to: "monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the increase in disruptive scam phone calls, texts, and emails he has received since the Data Breach." CAC ¶ 199.

Plaintiff Lackey's losses amounted to "significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation." CAC ¶ 199. He suffered: "(i) damage and loss of the value of his PII; (ii) loss of time; (iii) invasion of privacy; (iv) theft of his PII; (v) lost value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) fear of identity theft; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud." *See* CAC ¶ 200.

Lastly, Caesars erroneously contends that Lackey cannot bring this VCPA claim on behalf of a class. But "[t]he question of whether a class action may be maintained with respect to the [VCPA] is proper to consider at the class certification stage rather than in considering a motion to dismiss." *Mouzon v. Radiancy, Inc.*, 200 F. Supp. 3d 83, 90 (D.D.C. 2016); *Attias*, 518 F. Supp. 3d at 57 n.8. Even

at this stage, Caesars is incorrect that the VCPA precludes class-wide relief. *See Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 417 (2010) (Stevens, J., concurring) (noting that federal courts sitting in diversity apply state substantive law and federal procedural law). Courts have routinely found that the VCPA limitation on class-wide relief is procedural and therefore preempted by Rule 23. *See, e.g.*, *Attias v. CareFirst, Inc.*, 344 F.R.D. 38, 57 n.6 (D.D.C. 2023); *Tijerina v. Volkswagen Grp. of Am., Inc.*, 2023 WL 6890996, at *32 (D.N.J. Oct. 19, 2023); *Milisits v. FCA US LLC*, 2021 WL 3145704, at *12 (E.D. Mich. Jul. 6, 2021).

6. Plaintiffs Adequately Plead Their Minnesota Claims.

The Minnesota Consumer Fraud Act ("CFA") prohibits "[t]he act, use, or employment by any person of any fraud unfair or unconscionable practice,false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise." Minn.Stat. § 325F.69, where merchandise means "any objects, wares, goods, commodities, intangibles, real estate, loans, or services." Minn. Stat. § 325F.68, Subd. 2. Defendants argue that "Plaintiffs' claims are defective because they hinge entirely on allegations of fraud relating to "security and privacy measures,"[] but Caesars is not in the business of selling data security services." Mot. at 37, citing *Mekhail v. N. Mem'l Health Care*, 2024 WL 1332260, at *6 (D. Minn. Mar. 28, 2024); *Kuhns* 868 F.3d at 719 (8th Cir. 2017). However, to the extent Caesars implies that "the only viable data breach class action lawsuits would be those asserting claims against companies that sell data security services," other courts have rejected that theory as "nonsensical." *See Perdue*, 455 F. Supp. 3d at 772-72 (collecting data breach cases by non-data security companies under Minnesota CFA and parallel Missouri Merchandise Practices Act). Furthermore, in contrast to *Mekhail* and *Kuhns*, Plaintiffs here have alleged that Caesars' business is dependent on the collection and use of Plaintiffs' personally identifying information. CAC ¶¶ 220, 221, 235-238. Indeed, Caesars requires customers to entrust it with highly sensitive PII as a condition of joining its rewards program (CAC ¶¶4, 126, 135, 212, 236) because it then uses this PII to its own financial benefit in ways that are critical to its business, including "to operate our Caesars Rewards program;" "track you[] for our internal market research and analytics;" "protect and defend our rights;" "notify you about promotions and special offers." CAC ¶¶237, 238.

Plaintiffs similarly state a claim under the Minnesota Deceptive Trade Practices Act ("MDTPA"), which prohibits the use of "deceptive trade practices" in the course of business, vocation, or occupation. Minn. Stat. § 325D.44, subd. 1(2), (13), (14). Here, Plaintiffs have properly alleged that (1) Caesars failed to implement and maintain reasonable security and privacy measures; (2) failed to identify and remediate foreseeable privacy risks despite knowing the risk of cybersecurity incidents in the hotel industry; (3) failed to comply with common law and statutory duties requiring data security and misrepresented that it would and omitted that it did not; (4) misrepresented that it would protect Plaintiffs' PII, and omitted that it did not do so. CAC ¶¶ 518-521.

Defendant states that Plaintiffs claims must fail because only injunctive relief is permitted under the MDTPA. But Plaintiffs pleaded that they "seek all relief allowed by law, including injunctive relief." CAC ¶¶ 305 (a)-(f); 306, 527. Caesars continues to retain Plaintiffs' data and continues to have subpar data security practices, subjecting Plaintiffs PII to further breaches unless injunctive relief is granted. Defendant's own citation of *Mekhail* confirmed that the past collection of Plaintiff's data resulted in the possibility of future misuse, which was enough to allege the risk of future harm and support injunctive relief. *Mekhail*, 2024 WL 1332260, at *10; *see also MGM,* 638 F. Supp. 3d at 1200, 1205-06 (finding that MGM's continued retention of Plaintiffs' PII could only be remedied by a prospective injunction).

Caesars relies on decisions that rejected the threat of future harm based on allegations that the hackers could misuse of the breached data in the future, not that defendants had retained the data with continued insufficient data security. *See Perdue*, 455 F. Supp. 3d at 773 (rejecting claim for injunctive relief where risk of future harm alleged was that hackers may misuse the data in the future and where Defendant had removed malware that caused the breach); *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *27 (D.N.J. Dec. 16, 2021) (no risk of future harm where breach occurred against a third-party debt collector who was not in a direct relationship with Plaintiffs and did not retain their data.). Nor can Caesars rely on the supposed payment to the attackers as a basis to deny any future disclosure. Mot. at 38. Caesars itself, in its 8-K and breach

notification letters concede that while it has "taken steps to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee this result."[10]

7. Plaintiffs Adequately Plead the Illinois Statutory Claims.

Plaintiffs have alleged a likelihood of future harm pursuant to the Illinois Deceptive Trade Practices Act ("IDTPA") for the same reasons. Caesars continues to retain Plaintiffs' data and continues to have subpar data security practices, subjecting Plaintiffs PII to further breaches unless injunctive relief is granted *MGM,* 638 F. Supp. 3d at 1200, 1205-06 (D. Nev. 2022) (finding plaintiffs were entitled to an injunction based on defendants' continued possession of their data and risk of future breaches); *Mekhail v. N. Mem'l Health Care*, 2024 WL 1332260, at *10 (Defendants continued possession of Plaintiffs' data was sufficient to need for an injunctive to protect against future harm under IDTPA and MDTPA).

Second, Caesars argues that Plaintiffs have not alleged actual damages under the ICFA to confer standing. Mot. at 38. This ignores the case law and Plaintiffs allegations that of loss of time on mitigation efforts, out-of-pocket costs, damage and loss of the value of their PII, loss of benefit of the bargain, actual fraud, increased risk of fraud and identity theft, increased in spam calls, emails, and texts, CAC ¶¶ 49, 50, 51, 53, 59, 60, 61, 63,69, 70, 71, 72, 74, 80, 81, 82, 84, 90, 91, 92, 94, 100, 101, 102, 104, 109, 110, , 111, 113, 473, as well as allegations that they would not have purchased Caesars' services or hotel rooms had they have known of Caesars' deficient security. *Id.* at ¶¶ 52, 62, 73,83, 93, 103, 112. Courts have found that is sufficient to allege economic losses under Illinois law. *See Perdue*, 455 F. Supp. 3d at 761, 769 (time spent monitoring bank account to deal with effects of a data breach is enough to allege economic loss under Illinois CFA).

Third, Caesars states in two sentences that none of the Plaintiffs received, directly or indirectly, communication from the Defendant. The CAC alleges that Caesars required Plaintiffs to turn over their PII (¶¶46, 56, 66, 78, 88, 98, 107), which Caesars then uses to send Plaintiffs promotional materials to operate the Caesars Rewards programs. CAC ¶¶ 236, 237. Defendant's citation to *De Bouse*

[10] CAC ¶ 6; *see also* https://www.mass.gov/doc/assigned-data-breach-number-30726-caesars-entertainment-inc/download, last accessed Oct. 12, 2024.

is inapposite; there, Plaintiff brought a claim against the pharmaceutical company that had manufactured a drug her doctor prescribed her, but Plaintiff had no interaction with the Defendant. *De Bouse v. Bayer*, 235 Ill. 2d 544, 555 (2009).

8. Plaintiffs Adequately Plead Their New York GBL Claim.

Contrary to Caesars' claims, Plaintiffs allege that Caesars violated the N.Y. Gen. Bus. Law § 349 ("N.Y. GBL") by engaging in consumer-oriented conduct that is materially misleading and that caused Plaintiffs injury. *Voters for Animal Rights v. D'Artagnan, Inc.*, WL 1138017, at *7 (E.D.N.Y. Mar. 25, 2021). "[T]o qualify as a prohibited act under the statute, the deception of a consumer must occur in New York." *Goshen v. Mut. Life Ins. Co. of New York*, 774 N.E.2d 1190, 1995 (N.Y. 2002). Caesars does not dispute that its conduct is consumer oriented, nor that Plaintiffs are residents of New York. Caesars' conduct caused injury, including Plaintiffs out-of-pocket costs for credit monitoring, time spent on mitigation efforts, loss of the value of PII, loss of benefit of the bargain, lost opportunity costs, the heighted risk of identity theft and fraud, attempts at identity theft and fraud, and theft of PII . CAC ¶¶ 147, 148, 149, 150, 151, 152, 160, 161, 162, 164, 534. And Plaintiffs have pled that Caesars misrepresented its data security and omitted material information about its deficiencies. In *MGM* the Court upheld Plaintiffs' N.Y. G.B.L. claim based on similar alleged deceptive acts or practices by Defendant. *MGM,* 638 F. Supp. 3d at 1206; *see also In re Blackbaud, Inc.*, 2021 WL 3568394, at *12-13 (D.S.C. Aug. 12, 2021) (upholding plaintiffs' N.Y. GBL claim, based on allegations that defendants failed to implement reasonable security measures, misrepresented its security measures and did not reasonably secure Plaintiffs' PII).

Caesars misleadingly implies that all statutes without a private right of actions may not serve as a predicate for GBL §349 claims. That is incorrect. GBL § 349 claims are routinely predicated on violations of federal laws without a private action, particularly those that address deceptive conduct, including the FTC Act, 15 U.S.C. § 45. *See MGM,* 638 F. Supp. 3d 1175 at 1206. (holding that duties imposed by the FTC Act serve as a predicate for violations of the GBL § 349); *In re Marriott International, Inc. v. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 493 (D.Md. 2020) (same); *In re Blackbaud, Inc.*, 2021 WL 3568394, at *12-13 (N.Y. GBL claim upheld, which was partly predicated on Defendant's violations of the FTC Act, HIPAA, and COPPA). Indeed, New York courts specifically

interpret § 349 "by looking to the definition of deceptive acts and practices under [S]ection 5 of the Federal Trade Commission Act." *In re Marriott Int'l, Inc,* 440 F. Supp. 3d at 494 (citing *New York v. Feldman*, 210 F. Supp. 2d 294, 302 (S.D.N.Y. 2002)).

IV. CONCLUSION

The Court should deny Caesars' Motion to Dismiss in its entirety. If the Court grants any part of the Motion, Plaintiffs respectfully request leave to amend the Complaint.

DATED this 28th day of October, 2024.

Respectfully submitted,

KEMP JONES, LLP

/s/ Michael J. Gayan

Don Springmeyer, Esq. (#1021)
Michael J. Gayan, Esq. (#11135)
3800 Howard Hughes Parkway, 17th Floor
Las Vegas, Nevada 89169

Liaison Counsel

John A. Yanchunis
Morgan & Morgan
Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602

Douglas J. McNamara
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW, 5th Floor
Washington, D.C. 20005

Amy Keller
DiCello Levitt LLP
10 North Dearborn Street, Sixth Floor
Chicago, Illinois 60602

Interim Class Counsel

Jeff Ostrow
Kopelowitz Ostrow, P.A.
1 West Las Olas Blvd, 5th Floor
Ft. Lauderdale, Florida 33301

Plaintiff's Steering Committee Chair

James Pizzirusso
Hausfeld LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006

Gerard Stranch
Stranch, Jennings & Garvey, PLLC
223 Rosa L Parks Ave, Suite #200
Nashville, Tennessee 37203

Gary M. Klinger
Milberg Coleman Bryson Phillips
Grossman, PLLC
227 W. Monroe Street, Suite #2100
Chicago, Illinois 60606

Sabita J. Soneji
Tycko & Zavareei LLP
1970 Broadway, Suite 1070
Oakland, California 94612

Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that on the 28th day of October, 2024, I served a true and correct copy of the foregoing **PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT** via the United States District Court's CM/ECF electronic filing system to all parties on the e-service list.

/s/ Pamela McAfee
An employee of Kemp Jones, LLP